

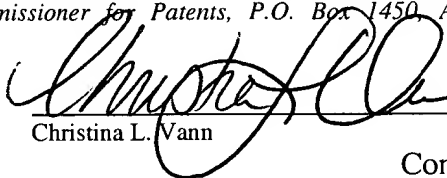


AF

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 13, 2006.


Christina L. Vann

Applicant : Craig L. Ogg, et al. Confirmation No. 1637
Application No. : 09/688,456
Filed : October 16, 2000
Title : CRYPTOGRAPHIC MODULE FOR SECURE PROCESSING OF
VALUE-BEARING ITEMS

Grp./Div. : 3621
Examiner : Firmin Backer

Docket No. : 39778/S850

APPELLANT'S BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Post Office Box 7068
Pasadena, CA 91109-7068
April 13, 2006

Commissioner:

Applicant, (hereinafter "Appellant") submits the following Appeal Brief pursuant to 37 C.F.R. § 41.37 for consideration by the Board of Patent Appeals and Interferences. Appellant also submits herewith a check in the amount of \$500.00 to cover the cost of filing the opening brief as required by 37 C.F.R. § 41.20(b)(2). Please charge any additional amount due or credit any overpayment to deposit Account No. 03-1728.

1. REAL PARTY IN INTEREST

Craig L. Ogg and William W. Chow, the parties named in the caption, assigned their rights to the invention disclosed in the subject application through an Assignment recorded on

Application No. 09/688,456

January 23, 2001 at reel 011462 and frame 0078 to Stamps.com, 3420 Ocean Park Boulevard, Suite 1040, Santa Monica, California 90405. Therefore, Stamps.com is the real party in interest.

2. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this Appeal.

3. STATUS OF CLAIMS

Claims 1-71 stand rejected. Appellant appeals the rejection of claims 1-71.

4. STATUS OF AMENDMENTS

No amendments to the claims were submitted after the Final Office Action mailed September 23, 2005.

5. SUMMARY OF CLAIMED SUBJECT MATTER

The subject matter of claim 1 relates to a cryptographic system for securing data on a computer network. See page 3, lines 9-11. The system includes a plurality of user terminals that are coupled to a computer network. Page 5, line 32 - page 6, line 4. A plurality of cryptographic devices that are remote from the user terminals are also coupled to the computer network. Page 7, lines 31-32. Each of the cryptographic devices include a processor programmed to authenticate a the plurality of remote users on the computer network for secure processing of a value bearing item; a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users; a cryptographic engine for cryptographically protecting data; an interface for communicating with the computer network, and a module for processing value for the value bearing item. See page 12, lines 21-23, page 24, lines 17-19 and page 7, lines 11-16.

Application No. 09/688,456

Each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users. Page 7, lines 8-9, page 8, lines 13-16, and page 11, lines 7-9. Additionally, each of the plurality of cryptographic devices is capable of processing a VBI printing request from any of the plurality of remote users; and of generating indicia data for transmitting to any of the plurality of remote users. See, for example, page 7, lines 8-9, page 8, lines 13-16, page 10, lines 32-35, and page 24, lines 17-20.

The subject matter of claim 41 relates to a method for securing data on a computer network including a plurality of users and a plurality of cryptographic devices remote from the plurality of users. See page 3, lines 9-11, page 5, line 32 - page 6, line 4, and page 7, lines 31-32. The method includes a series of steps such as authenticating any one of the plurality of remote users by any one of the plurality of cryptographic devices; and authorizing any one of the plurality of remote users for secure processing of a value bearing item by any one of the plurality of cryptographic devices. Page 7, lines 8-9, page 8, lines 13-16, and page 11, lines 7-9. Another step may be processing value for the value bearing item by any one of the plurality of cryptographic devices. See, for example, page 7, lines 8-9, page 8, lines 13-16, page 10, lines 32-35, and page 24, lines 17-20. A further step may include storing a security device transaction data in a memory for ensuring authenticity and authority of one of the plurality of users, wherein the security device transaction data is processed by any one of the plurality of cryptographic devices. Page 7, lines 8-16.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-71 are now rejected under 35 U.S.C. 102 (e) as being clearly anticipated by Lewis et al., U.S. 6,223,565 ("Lewis").

7. ARGUMENT

A. Rejection of Claim 1 under 35 U.S.C. §102 (e) as being anticipated by Lewis

Application No. 09/688,456

To establish a *prima facie* case of anticipation, the Examiner must establish that the cited reference teach every aspect of the claimed invention either explicitly or impliedly. In regard to claim 1, this claim includes the elements of "A cryptographic system for securing data on a computer network comprising: a plurality of users coupled to the computer network; and a plurality of cryptographic devices, each of the plurality of cryptographic devices remote from the plurality of users, and each of the plurality of cryptographic devices comprising: a processor programmed to authenticate the plurality of remote users on the computer network for secure processing of a value bearing item (VBI); a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users; a cryptographic engine for cryptographically protecting data; an interface for communicating with the computer network, and a module for processing value for the value bearing item, wherein each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users, wherein each of the plurality of cryptographic devices is capable of processing a VBI printing request from any of the plurality of remote users, and wherein each of the plurality of cryptographic devices is capable of generating indicia data for transmitting to any of the plurality of remote users." Appellant believes that the Patent Office has failed to establish that the cited reference teaches each of these elements of claim 1 and therefore has failed to establish a *prima facie* case of anticipation for claim 1.

In regard to the element of "a plurality of cryptographic devices, each of the plurality of cryptographic devices remote from the plurality of users," the system of Lewis dose not have a plurality of cryptographic devices remote from the plurality of users. Rather, Lewis describes a single cryptographic module (14) that is remote from the users. As illustrated in FIG. 1, Lewis discloses a remote service provider (RSP) 4, and a third party seller of goods and/or services (TPS) 6... . The client 2n has a Host system 10n and a PSD 20n which is resident on a [single] server of RSP 4. The Host 10n accesses the remote PSD 20n via the Internet 30." (Col. 6. lines

Application No. 09/688,456

39-59, emphasis added). The single server 4 comprises of its own single cryptographic module 14. (Col. 21, lines 64-65, emphasis added). Lewis further describes that each client 2n has its own cryptographic module 12. However, these client cryptographic modules 12 are not each "remote from the plurality of users." That is, at least one of the client cryptographic modules 12 is local to at least one user.

Regarding the element of "a module for processing value for the value bearing item," Lewis does not teach this element. Rather, in the system of Lewis, a Transaction Manager server 180 processes the value for all of the client transactions. See, for example, Col. 25, lines 5 -1, emphasizing that "once the client 2 has been authenticated, it submits a transaction request to the transaction server 180 and waits for a response. It now becomes the job of the Transaction Manager to process the transaction and return a "receipt" to the client 2. All transaction "receipts" will contain a date/time stamp, and a sequence number and a digital signature to verify the authenticity of a transaction" Therefore, "processing value" in Lewis is performed by the transaction server 180 and not by a module in each of a plurality of cryptographic devices.

Regarding the claimed element "wherein each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users," Lewis fails to teach this element. First, as mentioned above, the system of Lewis does not have a plurality of cryptographic devices remote from the plurality of users. Second, even if Lewis described a plurality of server cryptographic devices remote from the plurality of users, there is no description in Lewis that each of these imaginary server cryptographic devices is capable of authenticating any of the plurality of remote users. In fact, Lewis specifically describes that the cryptographic module 14 stores the Client Public Authentication Keys, which are used to prove the client's identity (that is, to authenticate the client), when a client attempts to establish a connection with the server 4. (Col 25, line 63-67. Also, see, Table III at the end of Col. 27, and col. 27, lines 58-59.).

Application No. 09/688,456

Therefore, even if Lewis had a plurality of server cryptographic devices remote from the users, each of those devices would not have been able to authenticate any of the plurality of users, because each cryptographic device would have had to maintain and update the Public Authentication Keys for all of the clients. There is no teaching in Lewis about this. Furthermore, each of the imaginary server cryptographic devices of Lewis would have had to be "stateless device, meaning that a PSD package can be passed to any device because the application does not rely upon any information about what occurred with the previous PSD package." (Specification, page 8, lines 13-16). Moreover, a PSD package for each of the imaginary server cryptographic devices would have had to include "all data needed to restore the PSD to its last known state when it is next loaded into a [different] cryptographic module." (Id., lines 22-24). There is no teaching in Lewis about this either.

Regarding the element "wherein each of the plurality of cryptographic devices is capable of processing a VBI printing request from any of the plurality of remote users," Lewis does not disclose this element. First, as mentioned above, the system of Lewis does not have a plurality of cryptographic devices remote from the plurality of users. Second, even if Lewis described a plurality of server cryptographic devices remote from the users, there is no description in Lewis that each of these server cryptographic devices is capable of processing a VBI printing request from any of the plurality of remote users.

Regarding the claimed element "wherein each of the plurality of cryptographic devices is capable of generating indicia data for transmitting to any of the plurality of remote users," Lewis falls short of teaching this element. First, as mentioned above, the system of Lewis does not have a plurality of cryptographic devices remote from the plurality of users. Second, even if Lewis described a plurality of server cryptographic devices remote from the users, there is no description in Lewis that each of these server cryptographic devices is capable of generating indicia data for transmitting to any of the plurality of remote users.

Application No. 09/688,456

Indeed, Lewis specifically describes that the cryptographic module 14 maintains the Client Private Indicium Keys, which are used to generating indicia data for that client. (Table III at the beginning of col. 28). Therefore, even if Lewis had a plurality of server cryptographic devices remote from the users, each of those devices would not have been able generate indicia data for transmitting to any of the plurality of users, because each cryptographic device would have had to maintain and update the Client Private Indicium Keys for all of the clients. There is no disclosure in Lewis about this.

Moreover, Lewis describes that "the first step to indicium generation is generating a public/private key pair for the server 4 [cryptographic module 14]. The public key is sent to the Certification Authority and a certificate for that server 4 is generated and returned to the Server. The Certification Authority also retains this certificate so that the Certification Authority can verify the authenticity of future server requests. Similarly, the server 4 will have a copy of the CA's certificate to verify the authenticity of data being sent back from the CA." (Col. 30, line 63 to col. 31, line 4). Consequently, the Certification Authority would have had to retain a different certificate for each of the imaginary server cryptographic devices to verify the authenticity of future server requests. There is no teaching in Lewis about this either.

Finally, each of the imaginary server cryptographic devices of Lewis would have had to be "stateless device and a PSD package for each of the imaginary server cryptographic devices would have had to include "all data needed to restore the PSD to its last known state when it is next loaded into a [different] cryptographic module." (Specification, page 8, lines 13-24). There is no teaching in Lewis about this either.

As a result, the Patent Office has failed to establish that the cited reference teaches each of the elements of claim 1 and therefore has failed to establish a *prima facie* case of anticipation for claim 1. Accordingly, it is requested that the anticipation rejection of claim 1 be overturned.

Application No. 09/688,456

In regard to claims 1-40, these claims depend from independent claim 1 and incorporate the limitations thereof. Thus, at least for the reasons mentioned above in regard to claim 1, these claims are not anticipated by the cited references. Accordingly, it is requested that the anticipation rejection of these claims be overturned.

Claim 41, includes elements similar to those of claim 1. Specifically, claim 29 includes the elements of " authenticating any one of the plurality of remote users by any one of the plurality of cryptographic devices; authorizing any one of the plurality of remote users for secure processing of a value bearing item by any one of the plurality of cryptographic devices; processing value for the value bearing item by any one of the plurality of cryptographic devices; and storing a security device transaction data in a memory for ensuring authenticity and authority of one of the plurality of users, wherein the security device transaction data is processed by any one of the plurality of cryptographic devices." Thus, the arguments set forth above in relation to the elements of claim 1, apply equally to these elements of claim 29. Accordingly, it is requested that the anticipation rejection of claim 41 be overturned.

In regard to claims 42-71, these claims depend from independent claim 41 and incorporate the limitations thereof. Thus, at least for the reasons mentioned above in regard to claim 41, these claims are not anticipated by the cited references. Accordingly, it is requested that the anticipation rejection of these claims be overturned.

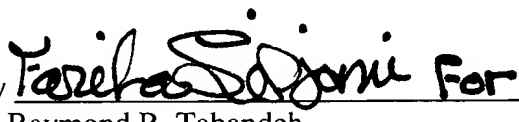
Application No. 09/688,456

Conclusion

Accordingly, it is submitted that the rejections of claims 1-71 based on 35 U.S.C. § 102(e) be overturned.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By  For
Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/clv

CLAIM APPENDIX

1. A cryptographic system for securing data on a computer network comprising:
a plurality of users coupled to the computer network; and
a plurality of cryptographic devices, each of the plurality of cryptographic devices remote from the plurality of users, and each of the plurality of cryptographic devices comprising:
a processor programmed to authenticate the plurality of remote users on the computer network for secure processing of a value bearing item (VBI);
a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users;
a cryptographic engine for cryptographically protecting data;
an interface for communicating with the computer network, and
a module for processing value for the value bearing item,
wherein each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users,
wherein each of the plurality of cryptographic devices is capable of processing a VBI printing request from any of the plurality of remote users, and
wherein each of the plurality of cryptographic devices is capable of generating indicia data for transmitting to any of the plurality of remote users.
2. The cryptographic system of claim 1, wherein the processor is programmed to verify that the identified user is authorized to assume a role and perform a corresponding operation.
3. The cryptographic system of claim 2, wherein the assumed role is a key custodian role to take possession of shares of keys.
4. The cryptographic system of claim 2, wherein the assumed role is an administrator role to manages a user access control database.

Application No. 09/688,456

5. The cryptographic system of claim 2, wherein the assumed role is a provider role to authorize increasing credit for a user account.

6. The cryptographic system of claim 2, wherein the assumed role is a user role to perform expected IBIP postal meter operations.

7. The cryptographic system of claim 1 further comprising a stored secret for cryptographically protecting data.

8. The cryptographic system of claim 1, wherein the secret is a password.

9. The cryptographic system of claim 1, wherein the secret is a public/private key pair.

10. The cryptographic system of claim 2, wherein the processor is programmed to include a state machine for determining a state corresponding to availability of commands in conjunction with the roles.

11. The cryptographic system of claim 1, wherein the processor is stateless.

12. The cryptographic system of claim 1, wherein the processor is programmed to prevent unauthorized and undetected modification of data.

13. The cryptographic system of claim 1, wherein the processor is programmed for preventing unauthorized disclosure of data.

14. The cryptographic system of claim 1, wherein the processor is programmed to ensure proper operation of cryptographic security and VBI related meter functions.

Application No. 09/688,456

15. The cryptographic system of claim 1, wherein the processor is programmed for providing indications of an operational state of a VBI meter.

16. The cryptographic system of claim 2, wherein the processor is programmed for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

17. The cryptographic system of claim 1, wherein the processor stores information about a number of last transactions in an internal register and compares the information saved in the register with the information saved in a memory before loading a new transaction data.

18. The cryptographic system of claim 17, wherein the memory includes data for creating indicium, account maintenance, and revenue protection.

19. The cryptographic system of claim 1, wherein the value bearing item is a postage value including a postal indicium.

20. The cryptographic system of claim 19, wherein the postal indicium comprises a digital signature.

21. The cryptographic system of claim 19, wherein the postal indicium comprises a postage amount.

22. The cryptographic system of claim 19, wherein the postal indicium comprises an ascending register of used postage and descending register of available postage.

23. The cryptographic system of claim 1, wherein the value bearing item is a ticket.

Application No. 09/688,456

24. The cryptographic system of claim 1, wherein the value bearing item includes a bar code.
25. The cryptographic system of claim 1, wherein the value bearing item is a coupon.
26. The cryptographic system of claim 1, wherein the value bearing item is currency.
27. The cryptographic system of claim 1, wherein the value bearing item is a voucher.
28. The cryptographic system of claim 1, wherein the value bearing item is a traveler's check.
29. The cryptographic system of claim 1, wherein each security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.
30. The cryptographic system of claim 1, wherein the processor is capable of sharing a secret with a plurality of other cryptographic devices.
31. The cryptographic system of claim 1, wherein the processor and the cryptographic engine generate a master key set (MKS).
32. The cryptographic system of claim 31, wherein the MKS includes a Master Encryption Key (MEK) used to encrypt keys when stored outside the device.

Application No. 09/688,456

33. The cryptographic system of claim 32, wherein the MKS further includes a Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device.

34. The cryptographic system of claim 31, wherein the MKS is exported to other cryptographic devices.

35. The cryptographic system of claim 1, further comprising a memory including a user profile for a subset of the plurality of users.

36. The cryptographic system of claim 35, wherein the user profile includes username, user role, password, logon failure count, logon failure limit, logon time-out limit, account expiration, password expiration, and password period.

37. The cryptographic system of claim 10, wherein the state machine comprises of an uninitialized state, an initialized state, an operational state, an administrative state, an exporting shares state, an importing shares state, and an error state.

38. The cryptographic system of claim 37, wherein the operational state comprises means for access control, means for session management, and means for key management, and means for audit support.

39. The cryptographic system of claim 1, wherein the cryptographic engine is programmed to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

40. The cryptographic system of claim 1, wherein at least one of the plurality of users is an enterprise account.

Application No. 09/688,456

41. A method for securing data on a computer network including a plurality of users and a plurality of cryptographic devices remote from the plurality of users, the method comprising the steps of:

authenticating any one of the plurality of remote users by any one of the plurality of cryptographic devices;

authorizing any one of the plurality of remote users for secure processing of a value bearing item by any one of the plurality of cryptographic devices;

processing value for the value bearing item by any one of the plurality of cryptographic devices; and

storing a security device transaction data in a memory for ensuring authenticity and authority of one of the plurality of users, wherein the security device transaction data is processed by any one of the plurality of cryptographic devices.

42. The method of claim 41 further comprising the step of printing the value bearing item.

43. The method of claim 41 further comprising the step of storing a plurality of security device transaction data in a database wherein, each transaction data is related to one of the plurality of users.

44. The method of claim 43 further comprising the step of loading a security device transaction data related to the cryptographic device when the user requests to operate on a value bearing item.

45. The method of claim 41 further comprising the steps of authenticating the identity of each user and verifying that the identified user is authorized to assume a role and to perform a corresponding operation.

Application No. 09/688,456

46. The method of claim 45, wherein the assumed role is an administrator role to manage a user access control.

47. The method of claim 45, wherein the assumed role is a provider role to authorize increasing credit for a user account.

48. The method of claim 45, wherein the assumed role is a user role to perform expected IBIP postal meter operations.

49. The method of claim 45, wherein the assumed role is a security officer role for initiating key management function.

50. The method of claim 45, wherein the assumed role is a key custodian role to take possession of shares of keys.

51. The method of claim 45, wherein the assumed role is an auditor role to manage audit logs.

52. The method of claim 41, further comprising the step of printing a postage value including a postal indicium.

53. The method of claim 52, wherein the postal indicium comprises a digital signature.

54. The method of claim 52, wherein the postal indicium comprises a postage amount.

55. The method of claim 52, wherein the postal indicium comprises an ascending register of used postage and descending register of available postage.

Application No. 09/688,456

- 56. The method of claim 41, further comprising the step of printing a ticket.
- 57. The method of claim 41, further comprising the step of printing a bar code.
- 58. The method of claim 41, further comprising the step of printing a coupon.
- 59. The method of claim 41, further comprising the step of printing a currency.
- 60. The method of claim 41, further comprising the step of printing a traveler's check.
- 61. The method of claim 41, further comprising the step of printing a voucher.
- 62. The method of claim 41, further comprising the step of storing a user profile for a subset of the plurality of users.
- 63. The method of claim 62, wherein the user profile includes username, user role, password, logon failure count, Logon failure limit, logon time-out limit, account expiration, password expiration, and password period
- 64. The method of claim 41, further comprising the step of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms by each of the cryptographic devices.
- 65. The method of claim 41, further comprising the steps of supporting multiple concurrent operators and maintaining a separation of roles and operations performed by each operator.
- 66. The method of claim 41, further comprising the steps of:

Application No. 09/688,456

storing information about a number of last transactions in a respective internal register of each of the one or more cryptographic devices;

storing a table including the information about a last transaction in the database;
and

comparing the information saved in the respective device with the respective information saved in the database.

67. The method of claim 66, further comprising the step of loading a new transaction data if the respective information stored in the device compares with the respective information stored in the database.

68. The method of claim 41, wherein the secret is a password.

69. The method of claim 41, wherein the secret is a public/private key pair.

70. The method of claim 41, wherein at least one of the plurality of users is an enterprise account.

71. The method of claim 41, wherein the security device transaction data is related to user authorization operations, user account operations, and VBI creation operations, and wherein each of the user authorization operations, user account operations, and VBI creation operations can be performed by any one of the plurality of cryptographic devices.

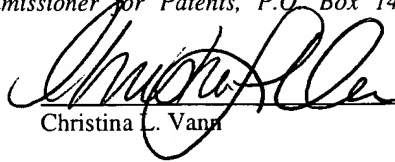
CLV PAS677120.1-* -04/13/06 9:53 AM



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 13, 2006.


Christina L. Vann

Applicant : Craig L. Ogg, et al. Confirmation No. 1637
Application No. : 09/688,456
Filed : October 16, 2000
Title : CRYPTOGRAPHIC MODULE FOR SECURE PROCESSING OF
VALUE-BEARING ITEMS
Grp./Div. : 3621
Examiner : Firmin Backer
Docket No. : 39778/S850

SUBMISSION OF APPELLANT'S BRIEF (1.192)
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Post Office Box 7068
Pasadena, CA 91109-7068
April 13, 2006

Commissioner:

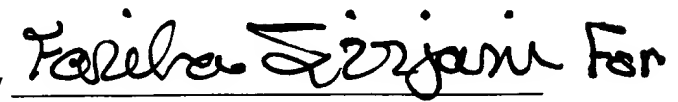
Enclosed for filing is the Appellant's Brief for this application.

 X Our check for \$500 to cover the fee for the appeal brief is enclosed.

The Commissioner is hereby authorized to charge any further fees under 37 CFR 1.16 and 1.17 which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account. **A copy of this letter is enclosed.**

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By 
Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900